REDACTED

Interoperability Showing Technical and Operational Response

State of Texas

Table Of Contents

Introduction

This Interoperability Showing Technical and Operational Response is intended to demonstrate the technical and operational proficiency of the State of Texas necessary to achieve operability and interoperability of public safety broadband networks in accordance with FCC Waiver Orders adopted on May 11, 2010, December 10, 2010, and January 25, 2011, docket number PS 06-229. The State of Texas will deploy a 700 MHz interoperable public safety wireless broadband network which is in compliance with these orders. A compliance summary is provided in Appendix E. Additionally, this showing is intended to demonstrate capabilities to comply with any and all future FCC rules and orders under said docket.

This interoperability showing addresses public safety broadband network covering the State of Texas. This network will be implemented in phases, whereby the first phase comprises the Harris County BIGNET project. As such, implementation details of the BIGNET project are included herein. The State of Texas intends to include additional vendors in subsequent phases of network implementation. Incorporation of additional vendors in subsequent implementation phases will follow the principles and practices described in this interoperability showing document, and hence will continue to comply with the FCC Waiver Orders referenced herein. The State of Texas will work closely with the Commission to insure that compliance is maintained through each phase of the deployment.

A. System Architecture

The Broadband Public Safety implementation is based on the 3GPP LTE standards, and consists of the Radio Access Network (RAN), the Evolved Packet Core (EPC), Devices, and the key interfaces exposed by these components. The implementation includes the ability to roam between systems, provide priority access and QoS to ensure the most critical public safety users receive the highest priority, and ensure the Broadband Public Safety implementation is secure.

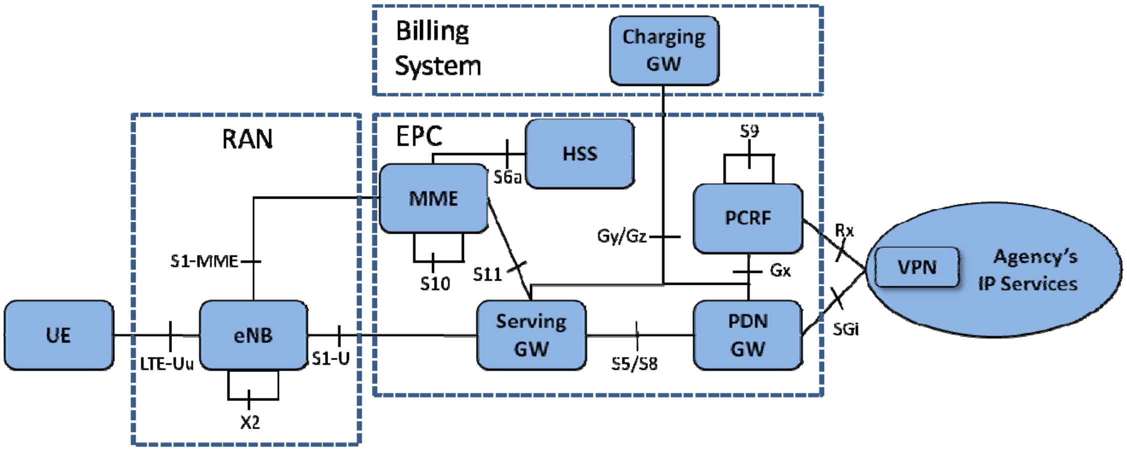


Figure 1 - Logical Architecture

The LTE RAN and EPC architecture and interfaces are shown in Figure 1 and described in the following sections. A more detailed description of the LTE/EPC infrastructure elements and interfaces is contained in Appendix B.

A.1 Radio Access Network (RAN) Architecture

The eNodeB (eNB) is the only 3GPP defined network element within the EUTRAN. The eNB provides the user plane and control plane protocol terminations toward the UE. The eNB consists of the inter-working function between the backhaul interface and the base band interface, the base band processing elements for the air interface, and the radios. The eNB in this system is compliant with the 3GPP Release 8 and Release 9 standards. The eNB is designed for compatibility with 3GPP compliant UE's and utilizes 3GPP compliant network interfaces.

Functions supported by an eNB are defined mainly in 3GPP Technical Specification (TS) 36.300. The RAN implementation for this system is compliant with specifications 36.211, 36.212, 36.213, 36.214, 36.300, 36.321, 36.322. 36.323, 36.331, 36.413, 36.423 and other referenced specifications. Compliance of devices and the RAN continues to evolve from 3GPP Release 8 specification versions and beyond. The eNB is designed to support upgrade to support modifications of the air-interface and network interfaces in accordance with evolution of the LTE standards.

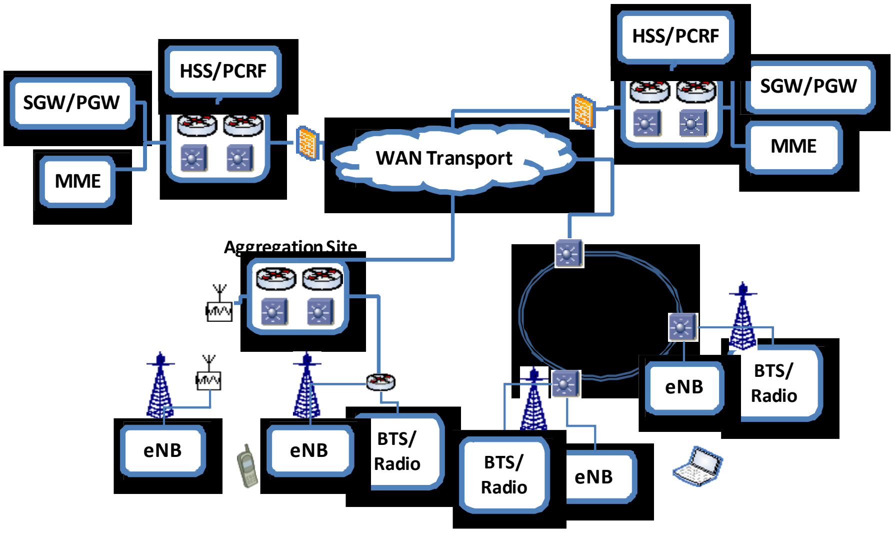


Figure 2 – RAN Physical Architecture

The RAN implementation is based on IP transport. The implementation supports collocation with existing narrowband or commercial sites and supports various types of backhaul transport mediums. The equipment supports the logical User Plane, Control Plane and OAM&P interfaces on the same physical interfaces and supports VLAN separation. The eNB hardware supports 5+5 MHz PSST band or 10+10 MHz D/PSST band or both D and PSST 5MHz bands simultaneously. The eNB is built with Self Organizing Network (SON) functions to automate deployment and optimization functions. The implementation will support both GPS and IEEE 1588v2 timing solutions as needed.

A.2 Core Network Architecture

The core network is based on the 3GPP R8 defined EPC (Evolved Packet Core) as mainly defined in 3GPP TS 23.401. The solution will support the MME, SGW, PGW, HSS and PCRF functions using standards-defined network interfaces. A VPN element is also shown. This element supports a secure public safety VPN and can be used with alternate access technologies (e.g., WiFi and 3G).

The EPC implementation is based on the GTP-based S5 and S8 interfaces. The EPC implementation is compliant with specifications 23.203, 23.401, 23.402, 24.301, 29.212. 29.214, 29.272, 29.274, 32.240, 32.251, 32.295 and other referenced specifications. Compliance of devices and infrastructure continues to evolve from 3GPP Release 8 specification versions and beyond.

Additional interfaces supporting charging are supported. The PGW and SGW can support both online (Gy) and offline (Gz) charging interfaces.

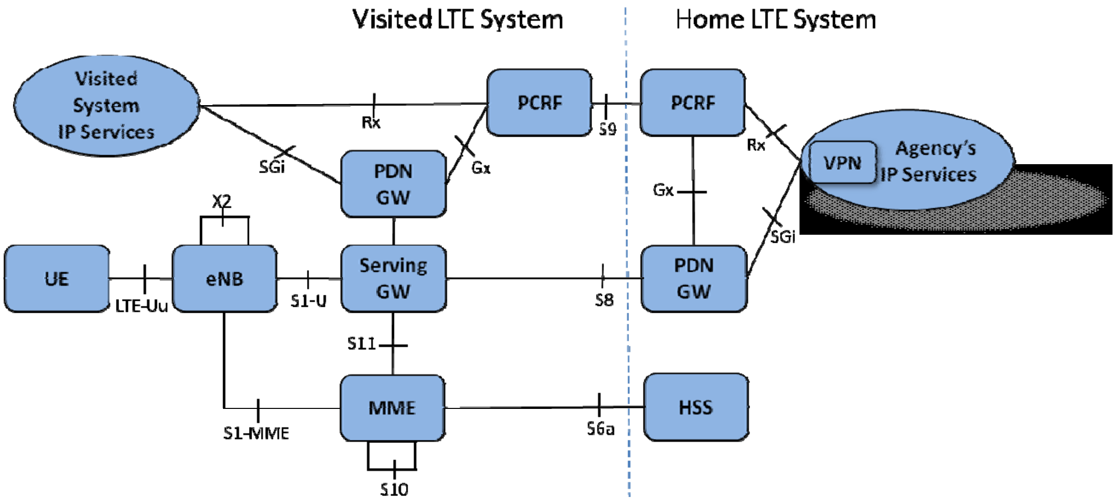


Figure 3 – EPC Roaming Architecture

The system is capable of supporting roaming with other regional PS LTE systems and with commercial LTE systems (if supported by the device capabilities).

The EPC physical architecture is shown in Figure 4. The EPC solution is based on IP transport and pooling of network elements. The solution supports IPv4 and IPv6 UE's and additional IPv6 network interfaces as a future software upgrade. Redundancy is supported at several levels including geographically distributed elements to mitigate disaster scenarios.

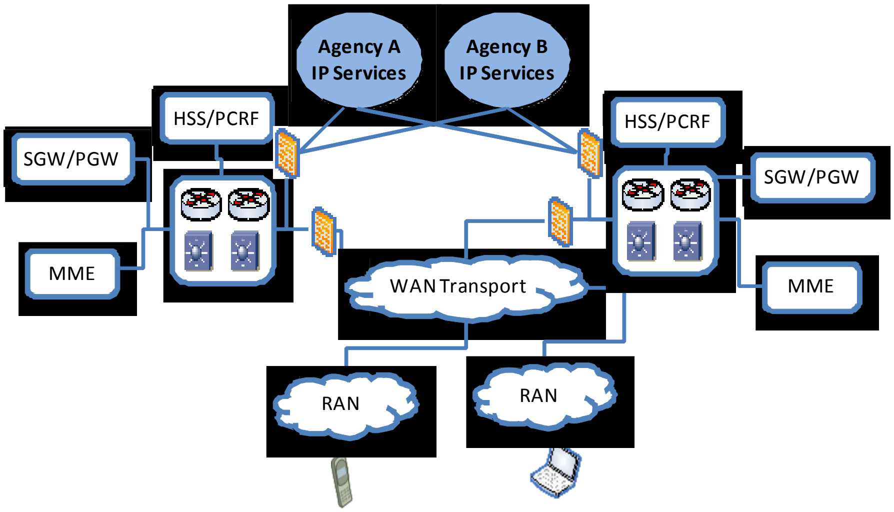


Figure 4 – EPC Physical Architecture

A.3 Interfaces

The RAN/EPC solution will support the following 3GPP interfaces:

LTE-Uu, Gx, Gy/Gz, Rx, S1-MME, S1-U, S5, S6a, S8, S9, S10, S11, SGi, X2

These interfaces support inter-operability of the LTE network with 3GPP R8 or R9 compliant UE devices, as well as inter-operability with other PS regional LTE networks. Details on handoff and mobility inter-operability are addressed in Section A.4 including mobility across regional PS LTE networks. Details on supporting a VPN service are also covered in Section A.4.

A.4 Mobility and Handoff (Handover)

Mobility and handover will be supported within the State of Texas and across the nationwide Shared Wireless Broadband Network (SWBN). These functions will be supported via 3GPP standardized interfaces. In addition, careful planning, configuration, optimization, and maintenance will be managed to achieve optimum handover performance. The mobility implementation accommodates both active and idle mode handovers within LTE networks. These aspects are discussed in more detail in the following paragraphs.

A.4.1 3GPP Compliant Handover

The mobility implementation is fully compliant with 3GPP standards. It supports high-speed mobility and seamless handoffs between eNBs within the Broadband Network. Radio frequency phase shift acquisition up to 300 Hz Doppler can be supported, which accommodates handoffs above 75 mph in a properly-engineered and maintained network.

The mobility implementation will support UE physical layer measurements, as specified in TS 36.214, to determine cell signal strengths and actions specified by the RRC L3 protocol in TS 36.331. The UE receives measurement control information from the eNodeB (eNB) via the following System Information Blocks (SIB):

- SIB3 information block contains common information for both intra-frequency and inter-frequency cell reselection
- SIB4 information block contains neighboring cell related information for intra-frequency cell re-selection including specific re-selection parameters
- SIB5 information block contains neighboring cell related information for inter-frequency cell re-selection including specific re-selection parameters

The MME and eNB utilize UE receiver measurement reports for controlling UE handover behaviors. When making a decision to handover a UE to another cell and/or carrier frequency the following factors or parameters are considered:

- UE measurement reports of its serving and neighbor cell signal strengths
- UE’s current signal to interference ratio
- UE’s serving cell and neighbor cell loading conditions
- UE’s QoS/application profile and the UEs mobility level

A.4.2 Adjacent Network Handover

The mobility implementation can support inter-network handover between regional public safety networks. The approach taken to support inter-network handover between regional networks is dependent on several factors. These factors include:

- Frequency bands assigned to and shared between the regional networks
- PLMN ID’s assigned to and shared between the regional networks
- Interfaces implemented across the regional networks
- Administrative relationships between the regional networks

If the regional networks are allocated a common frequency band, then issues associated with inter-band management are not required. However, if separate frequency bands are allocated to the regional networks, then inter-band handover management functions, such as neighbor band advertisement and frequency selection priority must be supported.

If all networks are allocated a common PLMN ID, then issues associated with inter-PLMN handover are avoided. However, in this case there must be a nationwide network planning, operations, and maintenance authority. The authority would be required to coordinate cell identifiers, eNB neighbor lists, network interconnections, and handover configurations across the regional administrative domains.

If the regional networks are allocated unique PLMN ID's (see section A.5) then inter-PLMN handover capabilities will be required as regional networks expand and become adjacent. In this case, nationwide network planning, operations, and maintenance are avoided. Instead, network planning and coordination is limited to RF planning along geographic borders between regions. The network interconnections are minimized and can leverage industry standard roaming interfaces.

The State of Texas is working with the public safety and vendor communities to deploy an interoperable implementation supporting adjacent network handover.

A.4.3 Mobile VPN

In addition to handover, the implementation also supports Mobile VPN (MVPN). MVPN implementations provide application-level session continuity across disparate radio access networks, as well as security between the UE and the agency application domain. Session continuity is supported at the application IP layer, which is above the radio access layer. Thus, the MVPN implementations can provide session continuity across various radio access technologies, such as LTE, 3G packet data, and Enterprise WiFi. Each radio access technology comprises an independent link between the MVPN server and the MVPN client in the UE. As such, each radio link is independently monitored and the optimum radio link is selected to support the application sessions. If a radio link becomes disconnected or impaired, the MVPN can switch to an alternate available radio link. Thus, the MVPN can provide IP layer mobility and intelligent route selection which is independent of handover in the radio access layer. The MVPN can provide a solution for mobility across disparate radio access networks.

In addition to providing IP layer mobility, the MVPN can provide secured connections between the server and client. The secured connection provides authentication, confidentiality, and integrity protection. Cryptographic modules which support the MVPN are compliant with FIPS 140-2 standards. The use of MVPN technologies with these security capabilities is critical, since current Criminal Justice Information Services (CJIS) security policy requires the use of highly secure VPNs for mobile device access.

A.5 Roaming

Roaming is the ability for a user to obtain service in a visited network. Roaming will be supported with other regional networks across the nationwide Shared Wireless Broadband Network (SWBN). These requirements are supported by leveraging 3GPP standardized interfaces, as well as adoption of a roaming services tailored to the SWBN.

A.5.1 PLMN ID Assignment

The NPSTC BBTF report recommends that the number of PLMN ID's allocated for the SWBN should be less than 100 IDs, and may be as few as 1 ID. The implementation will support this recommendation, and can be adjusted to accommodate the PLMN ID allocation for the SWBN. The State of Texas is working with the public safety and vendor communities to implement an interoperable PLMN ID assignment scheme. However, we recognize that national oversight authorities may require an alternative scheme, and thereby require reconfiguration of the State of Texas network, devices, and redeployment of SIM cards.

A.5.2 Intra-system Roaming

Intra-system roaming occurs when users obtain service from a visited regional network within the SWBN which is not the user's home network. The implementation will support intra-system roaming.

A.5.3 Inter-system Roaming

Inter-system roaming occurs when users obtain service from a commercial carrier network, which is not part of the SWBN. The implementation will support inter-system roaming as enabled by roaming agreements with one or more commercial carriers.

Commercial carriers typically leverage roaming service providers to provide inter-network connectivity, security, and billing functions. Roaming standards, such as IPX, are evolving to support QoS-enabled IP transport services, and therefore should support the services required for roaming with commercial carriers. However, inter-system roaming may have unique requirements as compared to commercial carrier roaming services, such as the support for a number of regional network entities comprising the SWBN. Therefore, it may be beneficial to establish an SWBN roaming service to minimally support intra-system roaming. In order to support inter-system roaming, the SWBN roaming service could then interface to commercial roaming service providers.

A.5.4 Roaming Interoperability

UE’s conforming to 3GPP standards will be able to roam across regionally deployed networks. However, it is essential for the UEs to be configured with appropriate frequency bands, PLMN lists, and access parameters corresponding to associated roaming agreements. 3GPP compliant UE’s will minimally support the following roaming-related behaviors:

- Scan supported/configured bands
- Perform network and cell selection
- Authenticate on a visited network

After authentication on a visited network, an IP address is assigned, and the UE then has the ability to access IP services. If home routed session is initiated, then the home network assigns an associated IP address to the UE. If a local breakout session is initiated, then the visited network assigns an associated IP address to the UE.

A.5.5 Roaming Configurations

The implementation will support home routed roaming configuration. Home routed configuration is when a user’s traffic is routed back to the home network to enable the use of home applications and Internet access. The home routed case can support the majority of Public Safety applications and use cases. Home routed bearer flows benefit from QoS policies controlled in the home network. In addition, home routed provides many operational and security benefits, such as:

- Single point of authentication for applications
- Single point for firewall, intrusion detection/prevention, and anti-virus protection
- Activity logging and Internet access policy control

The implementation will also support local breakout roaming configuration as needed for interoperability with future Public Safety applications. Local breakout configuration is when a user’s traffic is routed within the visited network, and therefore is not routed back to the user’s home network. Local breakout provides for optimization of bearer routing and access to visited network services. It should be noted that roamers may be subject to QoS policies of the local (i.e., visited) network.

A.6 Priority Access and QoS

LTE offers the most advanced QoS capabilities of any commercial cellular technology; however the technology must be properly configured for optimal public safety implementation. The State of Texas is working with the public safety and vendor communities to implement an interoperable priority access and QoS solution.. The implementation will be compliant with 3GPP TS 23.203.

A flexible priority access and QoS framework is provided by the implementation. Principles of the framework are as follows:

- **Regional Flexibility**
  Each public safety region has the flexibility to choose an LTE prioritization model to suit its need. For example, region 1 may prioritize responders based on role and region 2 may prioritize responders based on application. The region should have some latitude to choose how to prioritize devices and applications on the regional system.
- **Roaming Support**
  Whether roaming between regional systems or roaming to a commercial LTE system, the prioritization framework can support a consistent and fair policy of mapping priority between systems.

The realization of this framework includes adoption of LTE configuration parameters for public safety use, such as ARP, QCI, GBR, and MBR. Framework adoption must be consistent across all 700MHz public safety LTE systems in order to achieve meaningful interoperability.

A.7 Security

Security is a critical aspect of the public safety broadband network implementation. This section describes the comprehensive and interoperable security implementation in the State of Texas network.

Overall security architecture

3GPP standards have defined a suite of security related specifications for LTE systems. The 33 series of 3GPP specifications contains several documents defining various aspects of LTE and broadband application security architectures. From an interoperability perspective, of particular interest are the specifications 33.401 (“3GPP System Architecture Evolution (SAE); Security architecture”), 33.210 (“3G security; Network Domain Security (NDS); IP network layer security”), and 33.310 (“Network Domain Security/Authentication Framework (NDS/AF)”). The implementation will fully support the requirements stated in these specifications to ensure secure inter-system interoperability.

The implementation will support both the mandatory and optional aspects of the 3GPP SAE security architecture specification, as defined in 33.401. The optional aspects align with recommendations given by the NPSTC Broadband Task Force. Specifically:

- Both control plane and bearer plane traffic will be encrypted over-the-air. This includes RRC signaling, NAS signaling, and user plane traffic.
- Both SNOW 3G and AES encryption algorithms will be supported. AES will be default choice in the implementation, since it is a NIST/FIPS recommended algorithm for securing public safety communications.

The implementation will utilize secure O&M protocols and methods to distribute software and configuration information to the network elements.

Network Domain Security

The implementation will utilize the 3GPP defined mechanisms for Network Domain Security, as defined in the 3GPP spec 33.210, “Network Domain Security, IP Network Layer Security”. Per 33.210, the interfaces between the network entities in the network are to be secured using IPsec security associations. The security associations will be established and maintained using either IKE (Internet Key Exchange)v1 or IKEv2. Per 33.210, the Za interface is used to interface between two security domains and the Zb interface is used to interface between the various network entities within a single security domain. Specifically:

- NDS/IP inter-domain interface (Za) cryptographic protection via Security Gateways (SEGs) will be provided. The Za interface security associations will be established using IKEv1 or IKEv2. X.509 digital certificate based authentication will be utilized between SEGs in different security domains.
- NDS/IP intra-domain interfaces (Zb) as specified in 33.210 will be cryptographically protected unless within physically secure and/or fully trusted environments.

MVPN Access to Home

The Waiver Order requires petitioners' systems allow the use of network layer VPN access to any authorized site and to home networks on the deployed network. This requirement is designed to ensure the ability of first responders to securely connect back to their home systems when attaching to foreign wireless networks. Without this requirement, there is the risk some deployments may have their wireless networks configured to discard any traffic that is encrypted and destined to an external domain. This would be very problematic, as there are security compliance policies by CJIS, and NCIC (National Crime Information Center) that require the use of VPNs for remote user access.

CJIS (Criminal Justice Information System) requirements mandate the use of FIPS 140-2 validated encryption. Thus any user of a deployment utilizing a broadband waiver must use FIPS 140 validated implementations to be compliant with CJIS security policy and to access CJIS related services. The implementation will use FIPS 140-2 compliant VPN solutions for remote user access.

A.8 Devices

Delivery of user devices for Public Safety broadband agencies will be driven by the availability of LTE chipsets supporting standard 3GPP baseband protocols and RF operation in the 10 MHz of Public Safety spectrum (763 MHz to 768 MHz lower and 793MHz to 798 MHz upper). All devices will adhere to the 3GPP Release 8 or later air interface specification and the recommended out of band emissions (OOBE) as specified in the waiver order, as well as existing OOBE requirements to protect Public Safety narrowband voice services in the 700MHz spectrum. The following are examples of user devices intended for deployment in the State of Texas Public Safety LTE network:

USB-Modem

Initial trial and early deployment networks will be supported by a USB-modem device suitable for external connection to a host personal computer. A broad range of Public Safety legacy IP data applications including Internet, Mobile VPN, CAD, mobile office, text messaging, location, lookups, and records will be supported as well as uplink and downlink streaming video. The form factor of this device will follow commercial industry norms and be conducive to nomadic PC use both in and out of the vehicle. [redacted]

Vehicle Modem

The vehicle modem is an essential component for vehicle-based first responders and law enforcement officers in either urban/suburban or rural environments. The vehicle modem, equipped with a set of external high gain omni-directional MIMO antennas, offers improved link budget and throughput performance compared to embedded PC or USB solutions and is key to extending per site coverage range, particularly in rural environments. [redacted]

The vehicle modem will be suitably rugged for cab or trunk vehicle mounting and support Ethernet-based wired computers and peripherals. A broad range of Public Safety legacy IP data applications including Internet, Mobile VPN, CAD, mobile office, text messaging, location, lookups, and records will be supported as well as uplink and downlink streaming video from the vehicle.

Smartphone

A handheld device that serves as both a data and phone device is important to Public Safety LTE operations, particularly in urban/suburban environments where on-street or in-building portable coverage is provided. [redacted]

B. Applications

The FCC Waiver Order has identified a list of minimum applications that waiver networks must support. These applications provide the foundation for meaningful nationwide interoperability. This section will explain how the State of Texas network will support these applications.

B.1 Internet Access

Internet access will be hosted in Harris County. The implementation will support two methods to access the Internet: (1) by the responder's home system (i.e. home routed traffic) and (2) by the roamed-to (visited) system (i.e. local breakout). The UE selects an access point name (APN) identifier associated with the Internet Access host network and the MME determines whether the APN is for home routed or local breakout traffic. This is accomplished by either configuring a default APN in the subscribers HSS record or by requiring the Harris County APN to be programmed into the devices.

B.2 VPN Access to Any Authorized Site and to Home Networks

A secure VPN or MVPN may be implemented to support confidentiality and integrity of the responder's UE traffic. A corresponding device client may be necessary. A dedicated (M)VPN server may be deployed in an authorized site or in an agency home network, as the regional system dictates. An essential component of providing VPN access to any authorized site and to a home network is a network routing configuration which can support security, QoS, and network resiliency requirements. The State of Texas implementation will include support for each of these aspects.

B.3 Status/Information "Homepage"

The State of Texas network will provide the necessary functions to support the Status/Information Homepage (SIH) application. The SIH is envisioned to provide home and roaming responders with incident-specific information, alerts, system status, weather, traffic, and other information. This information may come from Computer-Aided Dispatch (CAD) terminals, responders, or in the future the NG911 ESInet.

The SIH builds upon the two previous (B.1, B.2) features. Access to the local SIH will be provided by way of Internet Access from the home system. All home and visiting users will obtain access to the SIH via the Internet access server. A well known URL (e.g., http://status.local.gov) will map to the Harris County SIH server.

In the future, the SIH may contain sensitive information and be accessed by many different responders (and roaming responders). Therefore, authorizations may be necessary to access certain SIH content. Because it is impractical for every SIH to contain subscription and authorization information for every public safety device in the U.S., a nationwide method will be eventually needed to provide federated identity management to a SIH server in a visited system. This capability can be layered onto the basic SIH access capability.

B.4 Access to Responders Under the Incident Command System

The National Incident Command System (NIMS) has defined an Incident Command System (ICS) to help quickly coordinate and organize mutual aid situations for typically large incidents. ICS offers many benefits including a command and control structure, common vocabulary, staging, incident action plan, and integrated communications.

Application servers used for Mutual Aid may be deployed in a variety of ways:

- by the region requesting mutual aid assistance
- by a hosting entity
- on the Internet
- by an on-scene command vehicle (see section B.5)

Regardless of deployment, applications used for ICS access (such as an ICS server or mutual aid communications service) must be accessible by both home and roaming UEs in the public safety region where the incident is taking place. It may also be necessary for responders outside the incident region to access the Mutual Aid application(s). This requires the public safety operators to support IP connectivity for each of these different application deployments and home/roaming devices. IP networking tools that can be deployed to support this application include:

- Static IP address assignments
- NAT/NAPT
- DNS
- IPv4v6 translation

The State of Texas network will provide the necessary functions to support the IP connectivity to application servers required to support the ICS application.

B.5 Field-Based Server Applications

Public safety today will deploy “command vans” and other tactical mobile vehicles to address specialized incidents, such as hurricanes. Typically, these vehicles use cellular technology as the “last mile” link for an application server co-resident in the command van. Similarly, the LTE air interface will serve as “last mile” for field-based application servers. These application servers must be accessible by:

- responders homed to the same public safety region as deploying the application
- roamers in the same public safety region as deploying the application
- responders homed in other public safety regions or carriers
- Internet users with authorization

In order to achieve this, HSS will be configured to allocate a static IP address to UEs serving as the modems for field-based servers. In order to be Internet-visible, this static IP address will use NAT/NAPT technology in the near term. Longer term, IPv6 technology may be used.

The State of Texas network will provide the necessary IP address allocation technologies to support the field-based server application.

C. Reliability and Availability

The implementation provides for high reliability and high availability for the following network components:

- Data Center and NOC
- LTE Enhanced Packet Core (EPC)

- Transport network
- Radio Access Network (RAN)
- Mobile and portable User Equipment

In addition, the implementation also includes support for a MVPN which enables use of diverse access technologies, such as WLAN and commercial carrier 3G networks. Please refer to section A.4.3 for additional information on the MVPN. The MVPN provides an additional level of disaster resilience by virtue of access to those networks, in that if a network becomes congested or goes down, Public Safety users will be able to obtain service on alternate surviving networks.

C.1 Regional Data Center and Network Operations Center

In order to maintain service availability, the network has been designed with multiple layers of redundancy and resiliency. The network can be deployed such that module failures, node failures, and even failure of an entire data center site will not degrade network service availability. The Regional Data Center and NOC can be deployed in a fully-redundant configuration, such that a catastrophic failure of a data center location will not result in the loss of critical functionality, since all operations and traffic can be served by an alternate data center.

Network elements are modular and fault tolerant, providing advanced high availability features. The high availability elements contain internally redundant components which include:

- Redundant data path switch fabrics
- Redundant control path switch fabrics
- Multiple power supplies using separate power feeds and buses
- Redundant network processing modules
- Redundant application processor modules

Server redundancy is supported. In the event of a server failure, redundant server nodes are invoked. High availability network elements include load balancing for application processing modules. In the event of a failure of a module, traffic will be distributed over the remaining active modules. Modules are hot swappable, with repair and replacement taking place without disruption of normal operations. The re-initiation of the configuration and software takes place upon replacement of the module prior to being placed into service.

C.2 Enhanced Packet Core

The EPC is comprised of the following standards-compliant network elements:

- Home Subscriber System (HSS)
- Policy and Charging Rules Function (PCRF)
- Serving Gateway (SGW)
- Packet Data Gateway (PGW)
- Mobility Management Entity (MME)
- Element Manager System (EMS)

These components are internally redundant and designed to provide robust hardware reliability and service assurance. The implementation is able to support EPC component pooling to achieve a highly available and resilient system with disaster recovery capabilities.

C.3 Transport Network

Transport network resiliency is accomplished by enabling a multi-path IP backbone network. As an analogy, the public Internet is highly available due to inherent mesh and/or ring connection of core routers. Additional resilience in the "last mile" links can be supported by deploying redundant links between the backbone and the network sites. Ethernet switches which comprise the transport nodes also use redundant hardware with dual homed switch ports. Failure of a switch or optical interface module will not result in the loss of traffic flow through the core network. If any failure of switches, links or modules occurs, traffic will be switched to a backup module or port. Interface redundancy allows backup links and ports. In addition, fiber rings can be leveraged to connect the cell sites and data centers. Agency networks are equipped with redundant links to the data centers.

C.4 Radio Access Network

The network site civil facilities are constructed according to industry best practice standards for:

- Building construction
- Seismic robustness
- Fire suppression
- Lightening and power surge protection
- Electromagnetic energy safety and interference management
- Power Utility service interconnect and backup power sources

The implementation includes site hardening standards which cover the design, construction, and maintenance aspects for each of these disciplines.

The implementation also leverages state-of-the-art system-on-chip (SoC) processors. These processors enable an exponential reduction of the number of chips and power consumption of electronic modules as compared to previous generation technologies. As a result, the Mean Time to Failure (MTTF) of electronic modules has increased significantly as compared to previous generation technologies. This has enabled a reduction in the number of redundant modules while maintaining required levels of service availability.

In addition, the implementation will include support for Cells on Wheels (COWS) provide coverage replacement and/or additional site capacity. This approach requires manual transport of the COWS to the target area. Therefore, this capability is targeted at planned events and large-scale incidents.

C.5 Mobile and Portable User Equipment

The mobile and portable User Equipment (UE) is hardened in accordance with Public Safety best-practices. Generally, the eco-system for LTE 700 MHz broadband Public Safety UE's is still emerging. However, we expect that as the eco-system matures, a wide range of device capabilities will be available to Public Safety markets, spanning low-end commercial grade devices to high-end devices compliant with military-specifications.

D. Radio Frequency (RF) Engineering

RF system performance factors such as coverage footprint, throughput, and capacity depend upon many different variables in RF design, including but not limited to the number of users, desired site density, system cost, and traffic model. These variables are interrelated, such that changes in one variable inevitably impact the others. The State of Texas system is designed to support users and applications in the most cost effective manner and the design is scalable for future expansion. The following paragraphs describe the tools and methodology used in designing this network.

D.1 Radio Access Network Planning

The State of Texas RAN design leverages extensive experience in modeling and designing wireless packet data networks, as well as extensive experience in RF propagation analysis.

The coverage prediction tools used in this analysis follow a two step process. First, an initial RF propagation analysis of the service area is performed using known models such as Okumura with shadow loss and TSB-88 statistical methods to provide a highly reliable prediction of coverage performance. Second, the tool performs a discrete event Monte Carlo simulation to model the LTE system based on operational requirements. This detailed simulation characterizes the system performance and interference analysis based on a particular number of users and a traffic model. Coverage maps are based on these simulation results, which depict coverage at certain performance levels. Coverage maps for the Harris County BIGNET deployment are provided in Appendix D of this document. Section D.1.4 of this document provides traffic model parameters.

D.1.1 RF Propagation analysis

The system is designed with coverage prediction tools, which were developed to provide an accurate prediction of radio coverage for a particular system by applying proven models to detailed system and environmental data across large geographical areas.

The system factors analyzed in the coverage modeling include: frequency, distance, transmitter power, receiver sensitivity, antenna height, and antenna gain. Environmental factors such as terrain variations, obstructions, vegetation, buildings, ambient noise, interference, and land-use in general are also taken into consideration for the analysis, using the data provided by environmental and topographical databases. Employing the knowledge gained from many years of practical experience and coverage testing, these coverage designs are performed by computing coverage, and throughput on every tile in a defined service area, thus providing the most accurate coverage prediction and reliability results.

D.1.2 Network Capacity and Throughput Analysis

The design methodology for the network was intended to meet, at a minimum, the current requirements of Harris County. However, it is recognized that over time State of Texas member agencies will require additional coverage. With these goals in mind, the Harris County BIGNET is designed to carry a certain amount of load per user per busy hour as explained in the “Modeling Assumptions” section D.1.4 below.

D.1.3 Scalability, expandability, and cost effective design

In any wireless network, the goals of coverage and capacity are intertwined and inversely proportional. Keeping in mind the conflicting needs of a cost effective design and high capacity, the network design methodology allows State of Texas member agencies the use of 4G type broadband applications while at the same time maximizing coverage from the available sites to ensure a cost effective implementation. This approach anticipates the current capacity requirements and ensures the ability to add further capacity with the addition of sites in the future. State of Texas anticipates the need for a larger number of sites over time. The network design offers a flexible approach starting with an affordable network deployment with a plan to build coverage and capacity as additional funding becomes available.

D.1.4 Modeling Assumptions

To date much of Public Safety wireless data usage has been limited to narrowband networks and few data points are available to shed light on Public Safety usage on LTE networks. While commercial wireless data usage has been increasing significantly in recent years, the more recent widespread use of smart phones has provided some insights into potential data consumption on LTE networks.

In order to arrive at a suitable broadband network profile for Public Safety, certain assumptions for traffic usage in the Harris County region has been made. The following parameters were also used for this design:

- 95% area reliability
- Coverage based on up to 4 HARQ retry attempts
- Mobile on street coverage using 23 dBm (200 mw) UEs
- 200 concurrent users per eNB
- Average cell edge data rates of 768 Kbps downlink and 256 Kbps uplink

- 14.9 dB antenna gain at the eNodeB
- Antennas heights ranging from 100-155 feet
- Single Frequency Reuse of the 10 MHz PSST spectrum in a 5+5 MHz configuration

A list of initial planned sites and coverage maps is provided in Appendix D of this document.

D.2 Interference Coordination

The implementation will employ several techniques and features to mitigate interference among Band 14 eNBs. These fall into two general categories: Network Planning and eNB Features. Note that Network Planning techniques may be applied to equipment from any vendor, and thus should be the first line of defense from an interoperability point of view. However, in a multi-vendor environment, eNB Features are dependent to some extent on compatibility of the vendor implementations. Thus it is possible that vendors of adjacent regions will be required to optimize and/or adapt their implementations for interference mitigation compatibility. Below are techniques and features which are planned to be employed in the system.

D.2.1 Network Planning

LTE system capacity and coverage performance depend on interference levels; therefore, interference mitigation is a primary objective of LTE RF system design. Several measures are taken during the system design phase to mitigate interference including selecting appropriate antenna patterns, adjusting the individual sector antenna tilts, and selecting optimal site locations and site separation distances.

D.2.1.1 Site Separation

An LTE system can be designed as noise limited or interference limited, depending on the separation distance between sites. In the case of a noise limited design, the coverage boundary is reached when the desired signal level is within a given threshold of the thermal noise floor. In contrast, when sites are deployed close together in a geographically contiguous manner, performance becomes limited by the co-channel interference as opposed to the thermal noise floor. The site separation distance also depends on the propagation environment and is selected to ensure that all coverage and interference requirements are met. Interference is attenuated more readily in environments where the propagation path loss slope is high and less readily in environments where the propagation path loss slope is low. The LTE design procedure and tools account for these differences in propagation environment as well as the noise limited versus interference limited considerations when determining the optimal site locations and separation distances.

D.2.1.2 Antenna Down-tilt

Down-tilting is the method of effectively adjusting the vertical radiation pattern of the antenna of the base station to direct the main energy downwards and reduce the energy directed towards the horizon. Down-tilting can be used to improve the level of coverage close to the site where "nulls" (e.g. coverage holes) may exist due to the effective height of the antenna. Down-tilting can also be used to reduce interference caused by reflections or undesired RF propagation beyond a predetermined footprint.

The final phase of the design process incorporates further detail into the design. This phase may include such items as collecting drive data to be used to tune or calibrate the propagation prediction model, and fine tuning of parameter settings, such as antenna down-tilting. This final design process is required in the deployment of a system. The main benefits of downtilting are:

- Control range of site
- Reduce energy at the horizon
- Maximize effective coverage closer to the site
- Reduce co-channel interference in adjacent sectors

The amount of down-tilt depends on the height of the antenna above the ground, the characteristics of the terrain, and the vertical beam-width of the antenna. The horizontal antenna beam width is selected to be narrow enough to limit interference between sectors yet wide enough to ensure reliable coverage. The vertical antenna beam width is selected to balance good coverage within the serving sector and interference mitigation to distant sectors. Antenna tilts are adjusted for each sector to optimize coverage within the serving sector while attenuating interference to distant sectors.

D.2.2 eNB Features

D.2.2.1 ICIC:

Inter-cell Interference Coordination (ICIC) is used as a means to improve coverage and edge of cell performance. Inter-cell interference techniques will be implemented in the State of Texas network. The goal is to achieve an evenly distributed utilization of radio resources between neighboring cells in low-to-medium loading scenarios, while also enabling high utilization of radio resources in high load scenarios.

D.2.2.2 Frequency Selective Scheduling:

OFDM systems can take advantage of the frequency selectivity of the uplink and downlink channels. Some frequency diversity gain may be achieved by varying subcarrier allocations over the entire carrier bandwidth. Additional diversity gain is possible by utilizing channel characteristics to allocate sub-band allocations that are favorable based on fading and/or interference conditions. The State of Texas may implement either or both of these Frequency Selective Scheduling techniques, depending on vendor-specific capabilities and deployment needs.

E. Testing

This section of the document describes the activities associated with testing which validates key functionality, performance and interoperability requirements of the PS LTE implementation. This is in addition to the extensive testing performed by the vendors in their internal laboratories to ensure conformance of their LTE implementation to 3GPP standards.

The State of Texas will insure that our vendors participate in the PSCR demonstration network. Trial activities will form the basis for initial testing of the system. This section provides an overview of the trial activities.

The trial lifecycle is broken into four stages: Site readiness, installation activities, interoperability testing, and test execution for specific functionality and applications.

Site Readiness: This includes all activities related to preparing the chosen site(s) for equipment installation. Site readiness begins after the sites have been identified for the trial.

Installation: This includes all activities related to installing the trial equipment. This stage is started once site readiness has completed and ends when all the equipment associated with the trial network has been installed. This stage also includes any testing to verify that the equipment was installed correctly.

IOT: This stage specifies the interoperability tests executed as part of the trial network. It includes all activities related to validating that other supplier components of the trial network are functioning correctly with our vendor’s components of the trial network prior to initiating trial testing.

There are two aspects of interoperability testing: 1) The Network, and 2) Devices. The network component validates that the other suppliers’ network elements are sufficiently functional with our selected supplier’s network components to initiate trial testing. The devices component validates that the devices used in the trial are sufficiently functional with our network components to initiate trial testing. The signaling procedures for the different interfaces will be tested using system level use cases. An example of use cases for the S1 interfaces is provided in the table below.

Figure 1.0 Example Interface Procedure to System Use Case Mapping – S1

Interface	Interface Specification Procedure	System Level Use Case
S1-MME	Reset	Link Management
	S1 Setup	
	Handover	S1 Based Handover
	E-RAB Setup, Modify, and Release	Dedicated Bearers
	Initial UE/Context	Attach, Detach, Authentication, TAU
	UE Context Request, Release Modification	Attach, Detach, Dedicated Bearer Procedures
	Uplink/Downlink NAS Transport, NAS Delivery/Error Indication	Attach, Detach, Authentication, TAU, Dedicated Bearer Procedures
S1-U	GTP Procedures	Link Management
	Bearer w/o Fragmentation	Uplink/Downlink Bearer Traffic
	Bearer with Fragmentation	Uplink/Downlink Bearer Traffic

The system level use cases that will be used to trigger and drive messaging for the IOT interfaces are detailed below:

S1-MME

- Link Management
- Attach
- Release
- Service Request
- Tracking Area Updates
- Detach
- Authentication
- Dedicated Bearers
- Handovers

S1-U

- Link Management
- Non-fragmented IP over GTP-U
- Fragmented IP over GTP-U

The majority of IOT activities related to the Uu (LTE radio) interface are conducted through vendor specific IOT testing in their labs.

Test Execution: This stage specifies the functional and performance tests executed as part of the trial. This stage is started once interoperability testing has completed. The following aspects will be tested:

- Inter-Node Communication Verification
- Operations and Maintenance (OAM)
- Single User Stationary Calls
- Multiple Users Stationary Calls
- Single User Throughput vs. Mobility

- Single User with QoS
- Multiple Users with QoS
- Multiple Users Mobility with QoS

As part of the goal to achieve nationwide interoperability, the following applications and interfaces will be tested as part of the trial activities, with testing distributed over time and as the technology matures (e.g., features are added) and the standards evolve. The applications and interfaces to be tested in the initial trial timeframe are described below. The interfaces that are in support of the required roaming model will be tested in two ways. Those interfaces that are part of the roaming feature will be tested in our supplier's internal laboratory environment. As systems are deployed in the field, and as we encounter other vendors' equipment outside of our home network, we will actively work to conduct the proper IOT testing with that agency (local or regional) and their supplier to verify the implementations. In this way we will address the fundamental roaming requirement and in testing the interfaces (visited to home) listed below.

Applications

- Internet access (Initial Trial)
- VPN access to any authorized site and to home networks
- Status or information homepage
- Access to responders under the Incident Command System
- Field-based server applications (Initial Trail)

Interfaces

- Uu-LTE air interface (Initial Trial)
- S6a-Visited MME to Home HSS
- S8-Visited SGW to Home PGW
- S9-Visited PCRF to Home PCRF
- S1-U-eNB to SGW
- S1-MME-eNB to MME

For the trial network, a configuration consisting of the following elements (in addition to tools and transport elements) will be used as the test bed: eNB, UE, MME, SGW, PGW, HSS, and PCRF. The software used in the test bed and as part of the verification trial is compliant to at least 3GPP Releases 8 of the LTE standard.

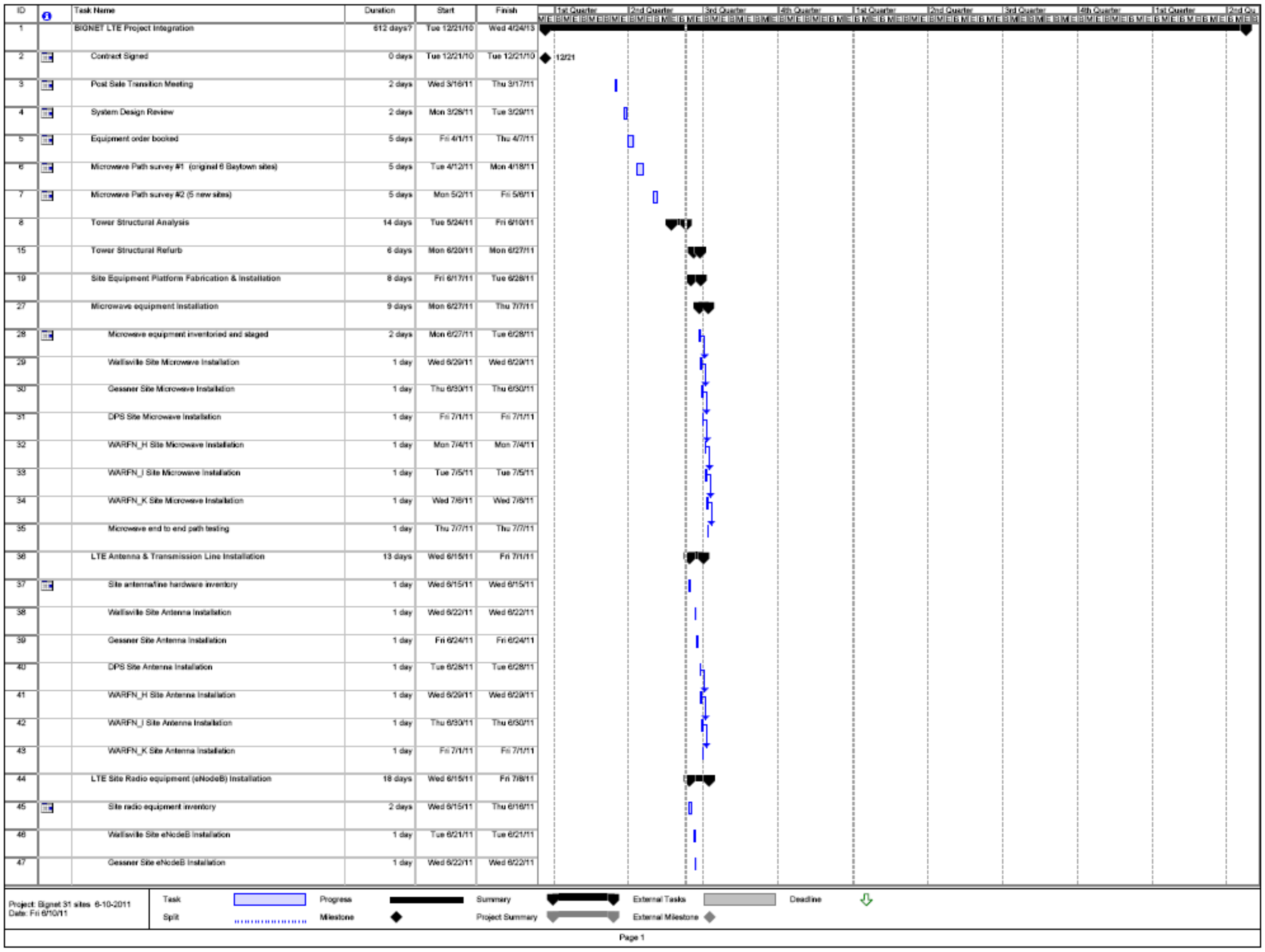
A listing of LTE test tools utilized by the implementation is included in Appendix C.

F. Deployment

The following project plan reflects a 31 site deployment which comprises the initial phase of deployment within the State of Texas. A .pdf format file is also embedded for expanded viewing.

Bignet 31 sites 6-10-2011.pdf

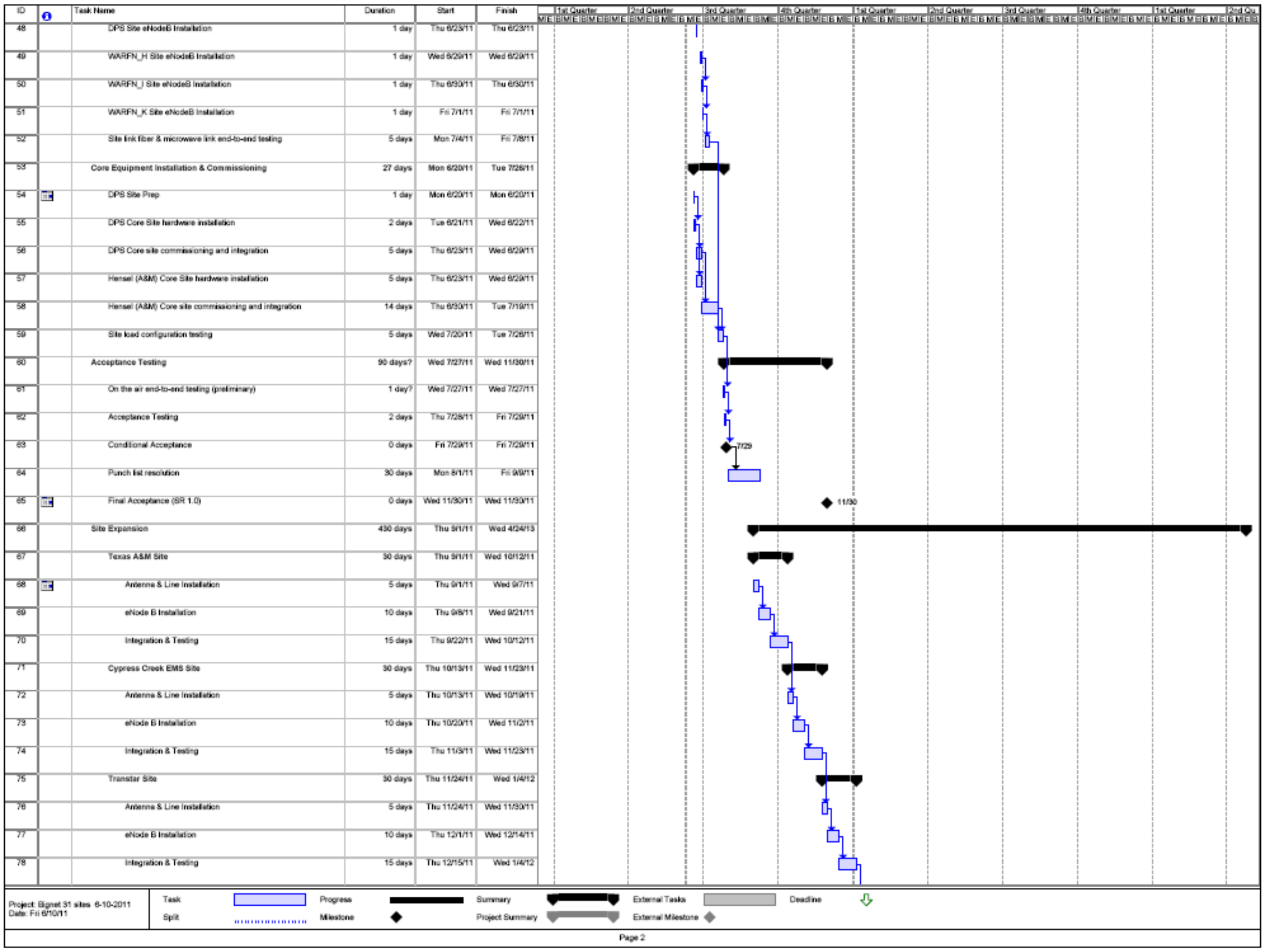
Subsequent deployment phases will be planned in accordance with requirements of the associated funding sources.



ID		Task Name	Duration	Start	Finish
1		BIGNET LTE Project Integration	612 days?	Tue 12/21/10	Wed 4/24/13
2		Contract Signed	0 days	Tue 12/21/10	Tue 12/21/10
3		Post Sale Transition Meeting	2 days	Wed 3/16/11	Thu 3/17/11
4		System Design Review	2 days	Mon 3/28/11	Tue 3/29/11
5		Equipment order booked	5 days	Fri 4/1/11	Thu 4/7/11
6		Microwave Path survey #1 (original 6 Baytown sites)	5 days	Tue 4/12/11	Mon 4/18/11
7		Microwave Path survey #2 (5 new sites)	5 days	Mon 5/2/11	Fri 5/6/11
8		Tower Structural Analysis	14 days	Tue 5/24/11	Fri 6/10/11
15		Tower Structural Refurb	6 days	Mon 6/20/11	Mon 6/27/11
19		Site Equipment Platform Fabrication & Installation	8 days	Fri 6/17/11	Tue 6/28/11
27		Microwave equipment installation	9 days	Mon 6/27/11	Thu 7/7/11
28		Microwave equipment inventoried and staged	2 days	Mon 6/27/11	Tue 6/28/11
29		Wallsville Site Microwave Installation	1 day	Wed 6/29/11	Wed 6/29/11
30		Gessner Site Microwave Installation	1 day	Thu 6/30/11	Thu 6/30/11
31		DPS Site Microwave Installation	1 day	Fri 7/1/11	Fri 7/1/11
32		WARFN_H Site Microwave Installation	1 day	Mon 7/4/11	Mon 7/4/11
33		WARFN_I Site Microwave Installation	1 day	Tue 7/5/11	Tue 7/5/11
34		WARFN_K Site Microwave Installation	1 day	Wed 7/6/11	Wed 7/6/11
35		Microwave end to end path testing	1 day	Thu 7/7/11	Thu 7/7/11
36		LTE Antenna & Transmission Line Installation	13 days	Wed 6/15/11	Fri 7/1/11
37		Site antenna/line hardware inventory	1 day	Wed 6/15/11	Wed 6/15/11
38		Wallsville Site Antenna Installation	1 day	Wed 6/22/11	Wed 6/22/11
39		Gessner Site Antenna Installation	1 day	Fri 6/24/11	Fri 6/24/11
40		DPS Site Antenna Installation	1 day	Tue 6/28/11	Tue 6/28/11
41		WARFN_H Site Antenna Installation	1 day	Wed 6/29/11	Wed 6/29/11
42		WARFN_I Site Antenna Installation	1 day	Thu 6/30/11	Thu 6/30/11
43		WARFN_K Site Antenna Installation	1 day	Fri 7/1/11	Fri 7/1/11
44		LTE Site Radio equipment (eNodeB) Installation	18 days	Wed 6/15/11	Fri 7/8/11
45		Site radio equipment inventory	2 days	Wed 6/15/11	Thu 6/16/11
46		Wallsville Site eNodeB Installation	1 day	Tue 6/21/11	Tue 6/21/11
47		Gessner Site eNodeB Installation	1 day	Wed 6/22/11	Wed 6/22/11

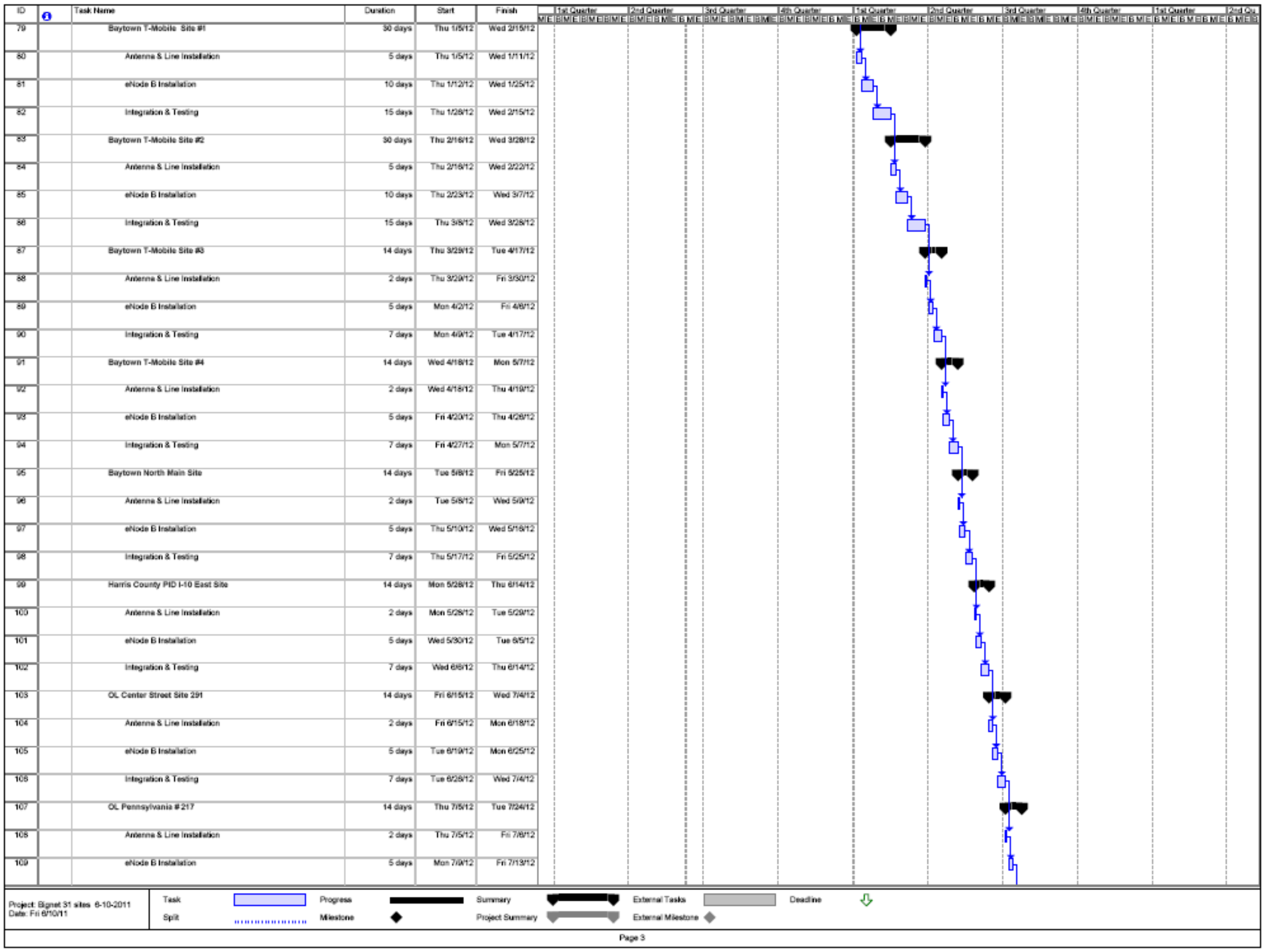
Project: Bignet 31 sites 6-10-2011
Date: Fri 6/10/11

Page 1



ID	ℹ	Task Name	Duration	Start	Finish
48		DPS Site eNodeB Installation	1 day	Thu 6/23/11	Thu 6/23/11
49		WARFN_H Site eNodeB Installation	1 day	Wed 6/29/11	Wed 6/29/11
50		WARFN_I Site eNodeB Installation	1 day	Thu 6/30/11	Thu 6/30/11
51		WARFN_K Site eNodeB Installation	1 day	Fri 7/1/11	Fri 7/1/11
52		Site link fiber & microwave link end-to-end testing	5 days	Mon 7/4/11	Fri 7/8/11
53		Core Equipment Installation & Commissioning	27 days	Mon 6/20/11	Tue 7/26/11
54	▦	DPS Site Prep	1 day	Mon 6/20/11	Mon 6/20/11
55		DPS Core Site hardware installation	2 days	Tue 6/21/11	Wed 6/22/11
56		DPS Core site commissioning and integration	5 days	Thu 6/23/11	Wed 6/29/11
57		Hensel (A&M) Core Site hardware installation	5 days	Thu 6/23/11	Wed 6/29/11
58		Hensel (A&M) Core site commissioning and integration	14 days	Thu 6/30/11	Tue 7/19/11
59		Site load configuration testing	5 days	Wed 7/20/11	Tue 7/26/11
60		Acceptance Testing	90 days?	Wed 7/27/11	Wed 11/30/11
61		On the air end-to-end testing (preliminary)	1 day?	Wed 7/27/11	Wed 7/27/11
62		Acceptance Testing	2 days	Thu 7/28/11	Fri 7/29/11
63		Conditional Acceptance	0 days	Fri 7/29/11	Fri 7/29/11
64		Punch list resolution	30 days	Mon 8/1/11	Fri 9/9/11
65	▦	Final Acceptance (SR 1.0)	0 days	Wed 11/30/11	Wed 11/30/11
66		Site Expansion	430 days	Thu 9/1/11	Wed 4/24/13
67		Texas A&M Site	30 days	Thu 9/1/11	Wed 10/12/11
68	▦	Antenna & Line Installation	5 days	Thu 9/1/11	Wed 9/7/11
69		eNode B Installation	10 days	Thu 9/8/11	Wed 9/21/11
70		Integration & Testing	15 days	Thu 9/22/11	Wed 10/12/11
71		Cypress Creek EMS Site	30 days	Thu 10/13/11	Wed 11/23/11
72		Antenna & Line Installation	5 days	Thu 10/13/11	Wed 10/19/11
73		eNode B Installation	10 days	Thu 10/20/11	Wed 11/2/11
74		Integration & Testing	15 days	Thu 11/3/11	Wed 11/23/11
75		Transtar Site	30 days	Thu 11/24/11	Wed 1/4/12
76		Antenna & Line Installation	5 days	Thu 11/24/11	Wed 11/30/11
77		eNode B Installation	10 days	Thu 12/1/11	Wed 12/14/11
78		Integration & Testing	15 days	Thu 12/15/11	Wed 1/4/12

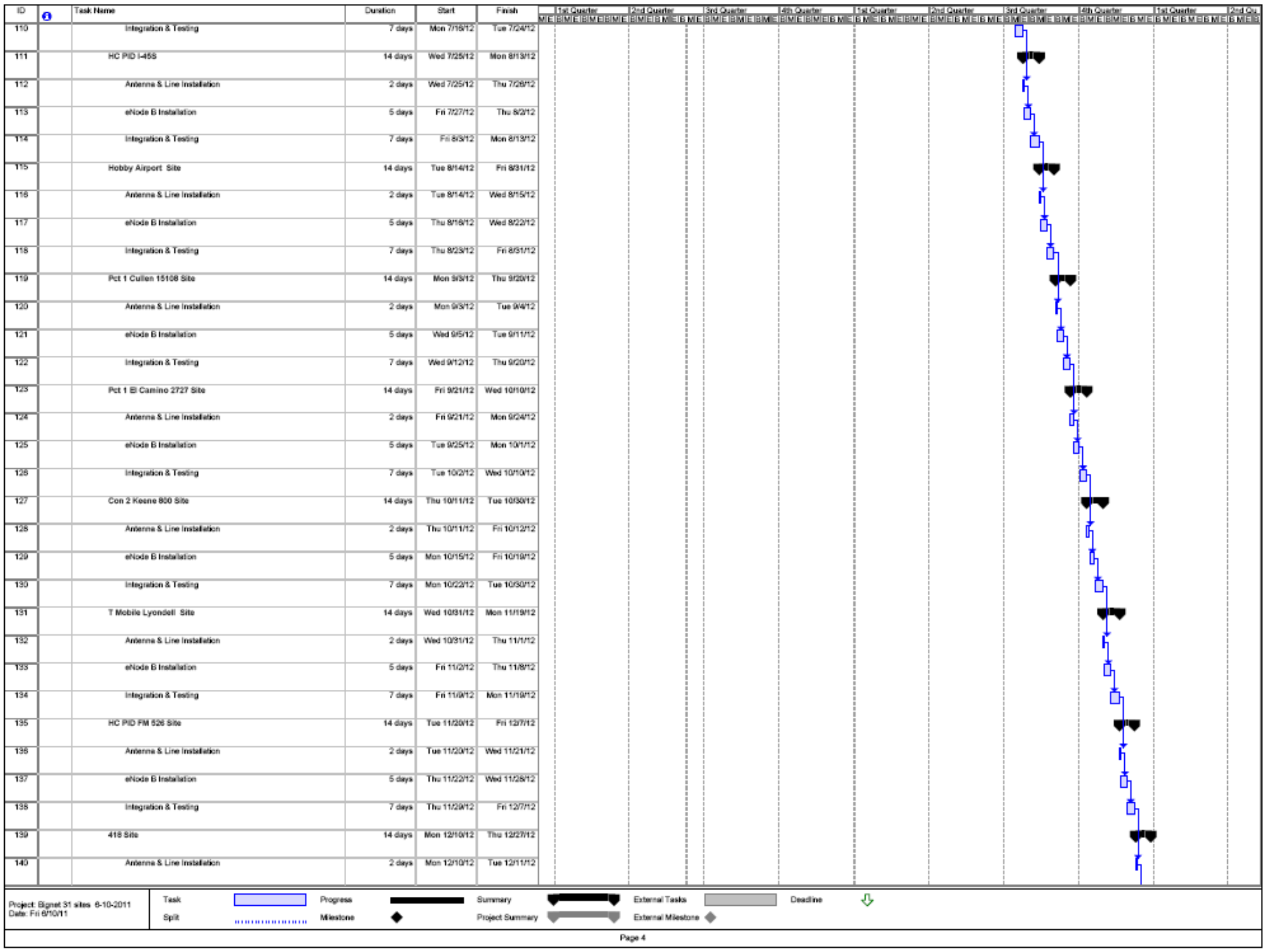
Project: Bignet 31 sites 6-10-2011
Date: Fri 6/10/11



ID	ℹ	Task Name	Duration	Start	Finish
79		Baytown T-Mobile Site #1	30 days	Thu 1/5/12	Wed 2/15/12
80		Antenna & Line Installation	5 days	Thu 1/5/12	Wed 1/11/12
81		eNode B Installation	10 days	Thu 1/12/12	Wed 1/25/12
82		Integration & Testing	15 days	Thu 1/26/12	Wed 2/15/12
83		Baytown T-Mobile Site #2	30 days	Thu 2/16/12	Wed 3/28/12
84		Antenna & Line Installation	5 days	Thu 2/16/12	Wed 2/22/12
85		eNode B Installation	10 days	Thu 2/23/12	Wed 3/7/12
86		Integration & Testing	15 days	Thu 3/8/12	Wed 3/28/12
87		Baytown T-Mobile Site #3	14 days	Thu 3/29/12	Tue 4/17/12
88		Antenna & Line Installation	2 days	Thu 3/29/12	Fri 3/30/12
89		eNode B Installation	5 days	Mon 4/2/12	Fri 4/6/12
90		Integration & Testing	7 days	Mon 4/9/12	Tue 4/17/12
91		Baytown T-Mobile Site #4	14 days	Wed 4/18/12	Mon 5/7/12
92		Antenna & Line Installation	2 days	Wed 4/18/12	Thu 4/19/12
93		eNode B Installation	5 days	Fri 4/20/12	Thu 4/26/12
94		Integration & Testing	7 days	Fri 4/27/12	Mon 5/7/12
95		Baytown North Main Site	14 days	Tue 5/8/12	Fri 5/25/12
96		Antenna & Line Installation	2 days	Tue 5/8/12	Wed 5/9/12
97		eNode B Installation	5 days	Thu 5/10/12	Wed 5/16/12
98		Integration & Testing	7 days	Thu 5/17/12	Fri 5/25/12
99		Harris County PID I-10 East Site	14 days	Mon 5/28/12	Thu 6/14/12
100		Antenna & Line Installation	2 days	Mon 5/28/12	Tue 5/29/12
101		eNode B Installation	5 days	Wed 5/30/12	Tue 6/5/12
102		Integration & Testing	7 days	Wed 6/6/12	Thu 6/14/12
103		OL Center Street Site 291	14 days	Fri 6/15/12	Wed 7/4/12
104		Antenna & Line Installation	2 days	Fri 6/15/12	Mon 6/18/12
105		eNode B Installation	5 days	Tue 6/19/12	Mon 6/25/12
106		Integration & Testing	7 days	Tue 6/26/12	Wed 7/4/12
107		OL Pennsylvania # 217	14 days	Thu 7/5/12	Tue 7/24/12
108		Antenna & Line Installation	2 days	Thu 7/5/12	Fri 7/6/12
109		eNode B Installation	5 days	Mon 7/9/12	Fri 7/13/12

Project: Bignet 31 sites 6-10-2011
Date: Fri 6/10/11

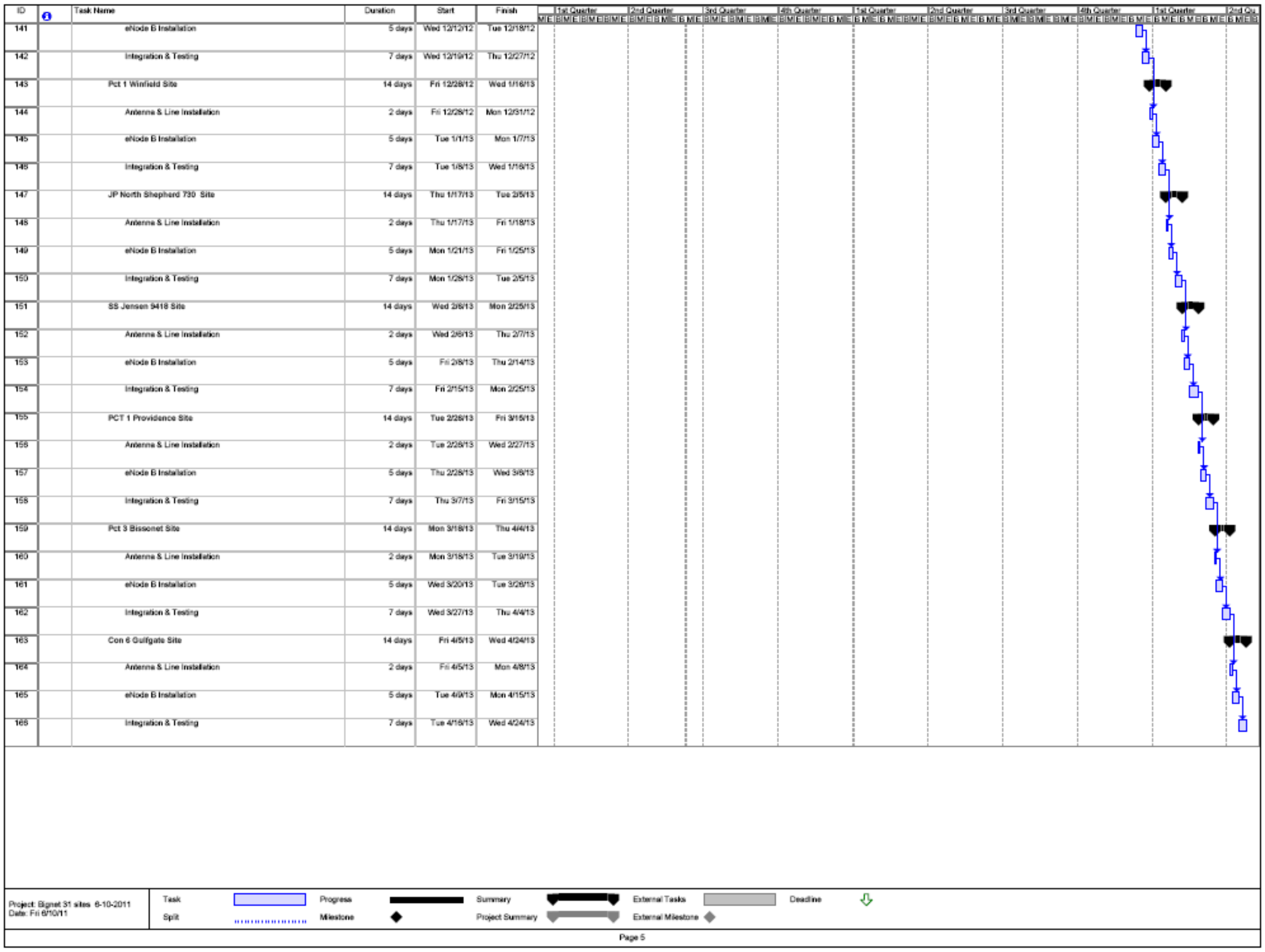
Page 3



ID	ℹ	Task Name	Duration	Start	Finish
110		Integration & Testing	7 days	Mon 7/16/12	Tue 7/24/12
111		HC PID I-45S	14 days	Wed 7/25/12	Mon 8/13/12
112		Antenne & Line Installation	2 days	Wed 7/25/12	Thu 7/26/12
113		eNode B Installation	5 days	Fri 7/27/12	Thu 8/2/12
114		Integration & Testing	7 days	Fri 8/3/12	Mon 8/13/12
115		Hobby Airport Site	14 days	Tue 8/14/12	Fri 8/31/12
116		Antenne & Line Installation	2 days	Tue 8/14/12	Wed 8/15/12
117		eNode B Installation	5 days	Thu 8/16/12	Wed 8/22/12
118		Integration & Testing	7 days	Thu 8/23/12	Fri 8/31/12
119		Pct 1 Cullen 15108 Site	14 days	Mon 9/3/12	Thu 9/20/12
120		Antenne & Line Installation	2 days	Mon 9/3/12	Tue 9/4/12
121		eNode B Installation	5 days	Wed 9/5/12	Tue 9/11/12
122		Integration & Testing	7 days	Wed 9/12/12	Thu 9/20/12
123		Pct 1 El Camino 2727 Site	14 days	Fri 9/21/12	Wed 10/10/12
124		Antenne & Line Installation	2 days	Fri 9/21/12	Mon 9/24/12
125		eNode B Installation	5 days	Tue 9/25/12	Mon 10/1/12
126		Integration & Testing	7 days	Tue 10/2/12	Wed 10/10/12
127		Con 2 Keene 800 Site	14 days	Thu 10/11/12	Tue 10/30/12
128		Antenne & Line Installation	2 days	Thu 10/11/12	Fri 10/12/12
129		eNode B Installation	5 days	Mon 10/15/12	Fri 10/19/12
130		Integration & Testing	7 days	Mon 10/22/12	Tue 10/30/12
131		T Mobile Lyondell Site	14 days	Wed 10/31/12	Mon 11/19/12
132		Antenne & Line Installation	2 days	Wed 10/31/12	Thu 11/1/12
133		eNode B Installation	5 days	Fri 11/2/12	Thu 11/8/12
134		Integration & Testing	7 days	Fri 11/9/12	Mon 11/19/12
135		HC PID FM 526 Site	14 days	Tue 11/20/12	Fri 12/7/12
136		Antenne & Line Installation	2 days	Tue 11/20/12	Wed 11/21/12
137		eNode B Installation	5 days	Thu 11/22/12	Wed 11/28/12
138		Integration & Testing	7 days	Thu 11/29/12	Fri 12/7/12
139		418 Site	14 days	Mon 12/10/12	Thu 12/27/12
140		Antenne & Line Installation	2 days	Mon 12/10/12	Tue 12/11/12

Project: Bignet 31 sites 6-10-2011
Date: Fri 6/10/11

Page 4



ID		Task Name	Duration	Start	Finish
141		eNode B Installation	5 days	Wed 12/12/12	Tue 12/18/12
142		Integration & Testing	7 days	Wed 12/19/12	Thu 12/27/12
143		Pct 1 Winfield Site	14 days	Fri 12/28/12	Wed 1/16/13
144		Antenna & Line Installation	2 days	Fri 12/28/12	Mon 12/31/12
145		eNode B Installation	5 days	Tue 1/1/13	Mon 1/7/13
146		Integration & Testing	7 days	Tue 1/8/13	Wed 1/16/13
147		JP North Shepherd 730 Site	14 days	Thu 1/17/13	Tue 2/5/13
148		Antenna & Line Installation	2 days	Thu 1/17/13	Fri 1/18/13
149		eNode B Installation	5 days	Mon 1/21/13	Fri 1/25/13
150		Integration & Testing	7 days	Mon 1/28/13	Tue 2/5/13
151		SS Jensen 9418 Site	14 days	Wed 2/6/13	Mon 2/25/13
152		Antenna & Line Installation	2 days	Wed 2/6/13	Thu 2/7/13
153		eNode B Installation	5 days	Fri 2/8/13	Thu 2/14/13
154		Integration & Testing	7 days	Fri 2/15/13	Mon 2/25/13
155		PCT 1 Providence Site	14 days	Tue 2/26/13	Fri 3/15/13
156		Antenna & Line Installation	2 days	Tue 2/26/13	Wed 2/27/13
157		eNode B Installation	5 days	Thu 2/28/13	Wed 3/6/13
158		Integration & Testing	7 days	Thu 3/7/13	Fri 3/15/13
159		Pct 3 Bissonet Site	14 days	Mon 3/18/13	Thu 4/4/13
160		Antenna & Line Installation	2 days	Mon 3/18/13	Tue 3/19/13
161		eNode B Installation	5 days	Wed 3/20/13	Tue 3/26/13
162		Integration & Testing	7 days	Wed 3/27/13	Thu 4/4/13
163		Con 6 Gulfgate Site	14 days	Fri 4/5/13	Wed 4/24/13
164		Antenna & Line Installation	2 days	Fri 4/5/13	Mon 4/8/13
165		eNode B Installation	5 days	Tue 4/9/13	Mon 4/15/13
166		Integration & Testing	7 days	Tue 4/16/13	Wed 4/24/13

Project: Bignet 31 sites 6-10-2011
Date: Fri 6/10/11

The State of Texas will provide the Commission with documented results of the IOT described in Section E on or before the conclusion of the 31 site deployment which comprises the initial phase of deployment. Further, the State of Texas will provide results of future IOT on or before the conclusion of each subsequent phase of the network build-out.

In accordance with FCC Order 10-2342, paragraph 16 and the deployment plan disclosed herein, the State of Texas hereby notifies the Bureau that a PLMN ID will be required for this network.

G. Operations, Administration and Maintenance

The OAM&P implementation is comprehensive and standards-based. It encompasses the entire lifecycle, including system design, assembly and staging, installation and commissioning, operations, optimization, and billing. The operations implementation includes Fault Management, Configuration Management, Accounting Management, and Performance Management (FCAPS) support for the system infrastructure and devices, as well as the following advanced capabilities:

Network Management System (NMS). The NMS provides an integrated point of control for the system. It includes network monitoring and recovery, security monitoring, performance management analysis and reporting, integrated configuration management, and infrastructure software upgrade.

Over The Air (OTA) Device Management. The Device Management implementation provides an easy-to-use interface to perform software upgrade, configuration and provisioning of a variety of public safety devices, including portables, vehicular modems, USB modems, and mobile data terminals.

Self Organizing Network (SON). The system SON implementation, fully based on 3GPP standards, provides a self-configuring, self-healing, and self-optimizing RAN implementation. System planning requirements are significantly reduced, as cell neighbors and LTE physical cell identifiers are automatically determined by the RAN infrastructure. Infrastructure equipment is automatically discovered and provisioned. The SON implementation should simplify emergency coverage such as Cell On Wheels (COW). Key features of the SON offering include:

- Automatic Neighbor Relations (ANR), which automatically determines the neighbors for each cell in the network, and continuously optimizes the neighbour lists.
- Automatic Physical Cell ID (PCI), which automatically computes the LTE physical cell identifier for each cell in the network.
- Base Station Integration Manager, which significantly simplifies planning, preparation, deployment and commissioning of eNBs.

Integrated Billing. The system provides an integrated billing implementation that supplies charging information, including the ability to support complex roaming and usage-based accounting. The billing implementation provides robust data analysis, reporting, invoicing and data warehousing.

OAM&P exhibits the following points of interoperability:

- The self-organizing network (SON) consists of use cases and interfaces defined by 3GPP and algorithmic processing to be defined by each vendor. If SON is utilized in LTE border cells, SON algorithm compatibility must be verified between vendors. Automatic Neighbor Relations (ANR) and Automatic Physical Cell ID (PCI) are two examples of SON algorithms that will need to be verified for interoperability between LTE vendors if LTE border cells enable these SON capabilities. A simpler option is to not enable SON capabilities in LTE border cells.
- Subscriber provisioning use cases and interfaces between the Public Safety Agency, Regional Public Safety Network and the Commercial Carrier Network must be formalized.
- Devices should be able to support OMA-DM clients in order to support standards-based device management implementations.
- Billing reconciliation between public safety LTE networks requires the exchange of billing records. Billing records will be exported and imported between networks using TAP3 record formats.

Appendices

Appendix A. Definitions and Acronyms

ARP	Allocation and Retention Priority
BBTF	Broadband Task Force
CAD	Computer Aided Dispatch
CJIS	Criminal Justice Information System
DNS	Domain Name Service
EPC	Enhanced Packet Core
E-RAB	EUTRAN Radio Access Bearer
FIPS	Federal Information Protection Standards
GPS	Global Positioning System
GTP	Generic Tunneling Protocol
HAAT	Height Above Average Terrain
HO	Handover
HSS	Home Subscriber Server
ICIC	Inter-Cell Interference Coordination
IKE	Internet Key Exchange
IOT	Inter-Operability Testing
IP	Internet Protocol
IPX	IP Exchange (see http://www.gsmworld.com/our-work/programmes-and-initiatives/ip-networking/ipi_documents.htm)
LTE	Long Term Evolution
MBMS	Multimedia Broadcast Multicast Service
MME	Mobility Management Entity
MVPN	Mobile Virtual Private Network
NAPT	Network Address and Port Translation
NAS	Non-Access Stratum
NAT	Network Address Translation
NCIC	National Crime Information Center
NOC	Network Operations Center
NPSTC	National Public Safety Telecommunications Council
OAM&P	Operations, Administration, Maintenance, and Provisioning
OMA-DM	Open Mobile Alliance – Device Management

OOBE	Out of Band Emissions
PC	Personal Computer
PCRF	Policy and Charging Rules Function
PDN	Packet Data Network
PGW	PDN Gateway
PKI	Public Key Infrastructure
PLMN ID	Public Land Mobile Network Identifier
PMIP	Proxy Mobile IP
PSST	Public Safety Spectrum Trust
PTT	Push To Talk
QCI	QoS Class Identifier
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technology
RFI	Request for Information
RICS	Regional Interoperable Communications System
SGW	Serving Gateway
SIB	System Information Block
SON	Self Organizing Network
TAU	Tracking Area Update
TS	Technical Specification
TSB	Telecommunications System Bulletin
UASI	Urban Area Security Initiative
UE	User Equipment
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

Appendix B. LTE/EPC Functions and Interfaces

This section provides a detailed description of the LTE RAN and EPC infrastructure elements, as well as their corresponding interfaces, and is provided as a supplement to sections A.1, A.2 and A.3.

eNB - The eNodeB (eNB) provides the user plane and control plane protocol terminations toward the UE. The eNB consists of the inter-working function between the backhaul interface and the base band interface, the base band processing elements for the air interface, and the radios.

- Radio Resource Management - Assignment, Re-assignment, and Release of radio resources
    - Radio Bearer Control (RBC) - Responsible for the Establishment, Maintenance, and Release of radio resources associated with specific radio bearers. The RBC function must maintain the quality of existing sessions when conditions change due to environmental and mobility activity.
    - Radio Admission Control (RAC) - Responsible for maximizing the radio resource utilization by intelligent admission or rejection of new radio bearer requests.
    - Connection Mobility Control (CMC) - Responsible for the management of radio resources during active or idle mode mobility of the UEs.
    - Dynamic Resource Allocation (DRA) - Packet Scheduler (PS) - Responsible for the scheduling of both user plane and control plane packets over the air interface. Scheduling takes into account QoS requirements of users, radio conditions, available resources, etc. to efficiently utilize the radio resources for all active users.
- MME Selection when UE initially attaches - A single eNB may have communication links to multiple MMEs. The controlling MME for each session must be selected if the UE does not indicate a specific MME to be used, or if the MME specified by the UE is unreachable.
- Routing user plane data to the SGW - A single eNB may have communication links to multiple SGWs. The data stream for each UE must be routed to the appropriate SGW.
- Scheduling and transmission of paging messages received from the MME.
- Scheduling and transmission of broadcast information received from the MME or configured from the Element Manager - The scheduling on the appropriate radio resource block and periodic broadcasting is performed by the eNB.
- Measurement gathering for use in scheduling and mobility decisions - Scheduling and handover decisions are performed based on uplink related measurement data from the eNB and downlink related measurement data from the UE. The eNB configures the measuring and reporting criteria and collects the data for input to the scheduling and handover functions.
- Radio Protocol Support
    - Radio Protocol Support
    - Physical Layer (Control and Bearer)
    - MAC (Control and Bearer)
    - RLC (Control and Bearer)
    - PDCP (Control and Bearer)
    - RRC (Control)

  - Session trace
- Inter-eNB handover preparation, Context & Buffer forwarding, Inter-cell interference coordination.
- eNB also forwards buffered downlink data during the Inter eNB handovers using non guaranteed delivery of user plane PDUs.

MME - The MME (Mobility Management Entity) manages authenticating users on the EPC and tracks active and idle users in the RAN. The MME pages users when triggered by new data arriving for an idle user at the assigned SGW. When a user attaches to an eNB, the eNB selects a serving MME. The serving MME selects a SGW and a PGW to handle the users bearer packets. The MME provides the following functions:

- Non-Access Stratum (NAS) Signaling. The MME is the termination point in the network for ciphering/integrity protection for NAS signaling and handles the security key management.
- Authentication: The MME is responsible for authenticating the UE by interacting with the HSS and is also responsible for the generation and allocation of temporary identities to UEs.
- Idle State Mobility Handling. The MME is responsible for idle mode UE tracking and paging procedure including retransmissions. The MME handles page request to its associated eNBs that contained the tracking area list last registered by the UE.
- EPC Bearer Control. The MME is involved in the bearer activation/deactivation process and is also responsible for selecting the SGW and PDN-GW for a UE at the initial attach, dedicated bearer activation, service request, and handover involving MME or SGW relocation.

SGW - The Serving Gateway terminates the S1-U interface towards EUTRAN and is also the local mobility anchor for the UE. The mobility anchor function applies to a mobile in the EUTRAN. For each UE associated with the Evolved Packet System (EPS), at any given point of time, there is a single serving SGW. The SGW maintains a packet buffer for each idle UE and holds the packets until the UE is paged and an RF channel is re-established. The SGW maintains a connection to a PGW for each UE. The SGW provides the following functions:

- Local Mobility Anchor point for inter-eNB handover
- Packet routing and forwarding
- Assist the eNB reordering function during inter-eNB handover by sending “end marker” packets to the source eNB immediately after switching the path
- E-UTRAN idle mode downlink packet buffering and initiation of network triggered service request procedure

PGW - The Packet Data Network Gateway (PGW) is the gateway which terminates the SGi interface towards the PDN (e.g. agencies network). The PGW is a macro mobility anchor and is responsible for UE address assignment. The PGW provides the following functions:

- The Packet Data Network Gateway terminates the SGi interface towards the PDN. The PGW supports connectivity of UE’s traffic to specified interfaces based on APN (Access Point Name). The APN determines which PDN a UE is connected to.
- UE IP address allocation, DHCPv4 (server and client) and DHCPv6 (client, relay and server) functions
- The PGW is the source of service data flow based charging records for the UE.
- The PGW acts as the macro mobility anchor for the UE across EUTRAN.

- UL and DL bearer binding and UL bearer binding verification.
- Transfer of (QoS) policy and charging rules from PCRF to Policy and Charging Enforcement Function (PCEF) in the PGW. Policing and shaping the traffic rate of the user's downlink EPS bearers.
- Transport level packet marking in the uplink and downlink, e.g. setting the DiffServ Code Point, based on the QCI of the associated EPS bearer.

HSS – The HSS stores UE subscription and authentication data for authenticating/authorizing UE access. The HSS provides the following functions:

- Authentication and authorization data for the UE
- Location information of the UE (MME and PGW serving the UE)
- Lawful intercept support
- The HSS in the implementation shares the UE subscriber database with the PCRF

PCRF - The PCRF provides network control regarding the service data flow detection, gating, QoS authorization and flow based charging (except credit management) towards the network element. The PCRF supports dynamic interfaces towards applications and a rule based engine that allows policy rules to be executed and the resulting policy passed to the PGW. The PCRF can pass both QoS and charging rules to the PGW. The PCRF stores subscription profile records and provides the following functions:

- PCRF decides how service data flows will be treated in the PGW, and ensures that the PGW user plane traffic mapping and treatment is in accordance with the user's subscription profile.
- PCRF will check that the service information is consistent with both the operator defined policy rules and the related subscription information. Service information will be used to derive the authorized QoS for the service.
- PCRF authorizes QoS resources. The PCRF uses the service information and/or the subscription information to calculate the proper QoS authorization (QoS class identifier, bit rates, etc.).
- PCRF can use the subscription information as basis for the policy and charging control decisions.
- PCRF supports different bearer establishment modes (UE-only, UE/Network or Network-only).

Supported Interfaces:

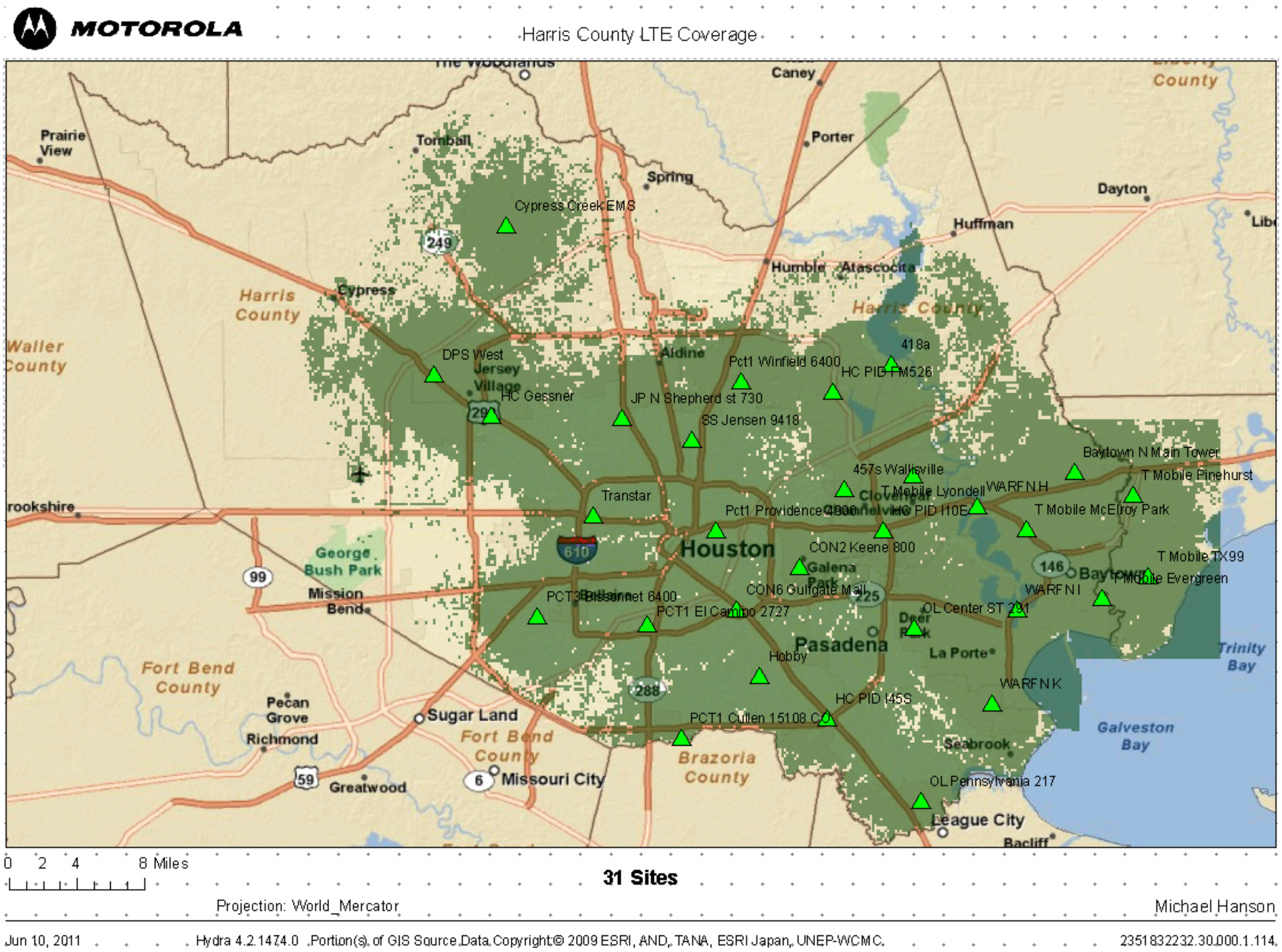
- **LTE-Uu** - This interface carries control and user (bearer) signaling between the eNB and the UE to facilitate the delivery of high speed data services to the end user. The associated control plane signaling supports mobility management, session management, admission control, QoS management, radio resource/connection management and all other functions that are necessary to enable the transfer of application data across the user plane.
- **Gx** - Provides transfer of (QoS) policy and charging rules from PCRF to the PGW.
- **Gy/Gz** - This interface is based on the GTP prime protocol. It is used to transfer Charging Detail Records (CDRs) from a PGW and/or SGW to a Charging Gateway in support of online/offline charging.
- **Rf/Ga** - This interface based on the DIAMETER protocol. It is used to transfer Charging Detail Records (CDRs) from a PGW and/or SGW to a Charging Gateway in support of offline charging.

- **Rx** – This reference point enables transport of application level session information from application to PCRF. Such information includes IP filter information to identify the service data flow and Media/application bandwidth requirements for QoS control.
- **S1-MME** - Control plane signaling between the eNB and the MME
- **S1-U** - Bearer plane support between the eNB and the SGW. In general, procedures for the S1-MME interface may affect the setup or teardown of a bearer link; however, the standards do not indicate specific procedures between the eNB and SGW. This path interface is for uplink and downlink data only.
- **S5** - The S5 interface provides user plane tunneling and tunnel management between SGW and PGW. It is used for SGW relocation due to UE mobility and if the SGW needs to connect to a non-collocated PGW for the required PDN connectivity.
- **S6a** - This interface enables the transfer of subscription and authentication data used for UE access to the LTE system. It carries control messages between the MME and the HSS over DIAMETER.
- **S8** – Roaming version of S5 for communication between a visited SGW and a home PGW.
- **S9 –** The S9 interface is between a home PCRF and a visited PCRF in the case of local breakout.
- **S10** - This interface carries control messages between MMEs.
- **S11** - This interface carries control messages between the MME and the SGW.
- **SGi** - This interface carries bearer traffic between the UE and the agencies PDN. This interface optionally carries control traffic between the PGW and the agencies PDN to facilitate IP address allocation, IP parameter configuration and AAA services associated with UE activity.
- **X2** - The X2 interface provides a control plane and bearer plane connection between eNBs to support load management and handover procedures.

Appendix C. LTE Test Tools

LTE Test Tools		
Function	**Tool (specified or equivalent)**	**Description**
Spectrum Analyzer	Agilent SA	Cell coverage, characteristics
Air Interface Monitor	UE Tool	Synchronization, system broadcast information, registration, DL/UL transfers
	Sanjole WaveJudge	
Network Monitor	Wireshark – Windows PC	Protocol dissectors to analyze L1/L2/L3, per segment
Service Simulator	Iperf – Windows PC	Service emulator using TCP and UDP pseudo packets and setting up bearer types and QoS over the air
Service Evaluator	Wireshark – Windows PC	Transport Quality (Loss, Latency, Jitter, Throughput), Handover Latency
UE	Available UE	Will be provided

Appendix D. Harris County Initial Phase Coverage Map



The above coverage map comprises 31 sites using the Application Model of 256 Kbps uplink and 768 Kbps downlink. The model parameters include 200 users per site at 95% covered area reliability for on-street portable devices.

Appendix E. Orders Compliance Summary

	Requirement	Orders	Compliance
1	Deploy LTE Release 8	10-79 §38 11-6 §10	Comply
2	Coordinate interference with bordering jurisdictions	10-79 §42	Comply
3	Devices support B14 5MHz	10-79 §47	Comply
4	Honor roaming requests	10-2342 §10	Comply
5	Submit, at least ninety days prior to its date of service availability, notice to the Bureau of its need for a PLMN ID for its network	10-2342 §10	Comply
6	[Support] … backward compatibility between all subsequent releases from Release 8 and onwards	11-6 §11	Comply
7	… compliance with Release 8 or higher of 3GPP standards prior to the date it achieves service availability.	11-6 §12	Comply
8	… remain subject to existing technical rules, the requirements of the *Waiver Order* and *Interoperability Waiver Order*, and the *new requirements adopted in this Third Report and Order*, and *future rules that may be adopted* in this proceeding.	11-6 §14	Comply
Interface Support (from day one of service operation)			
9	Uu	10-79 §47 10-2342 §11 11-6 §12	Comply
10	S6a	10-79 §47, 10-2342 §11 11-6 §12	Comply
11	S8	10-79 §47 10-2342 §11 11-6 §12	Comply
12	S9	10-79 §47 10-2342 §11 11-6 §12	Comply
13	S10 for Cat 1 Handover	10-79 §47 10-2342 §11 11-6 §12	Comply
14	X2	10-79 §47 10-2342 §11 11-6 §12	Comply
15	S1-U	10-2342 §12 11-6 §12	Comply
16	S1-MME	10-2342 §12 11-6 §12	Comply

17	S5	10-2342 §12 11-6 §12	Comply
18	S11	10-2342 §12 11-6 §12	Comply
19	SGi	10-2342 §12 11-6 §12	Comply
20	Gx	10-2342 §12 11-6 §12	Comply
21	Rx	10-2342 §12 11-6 §12	Comply
22	Gy/Gz	10-2342 §12 11-6 §12	Comply
Roaming and Security			
23	Roaming, Home Routed	10-79 §45 10-2342 §9	Comply
24	Roaming LBO	10-79 §45 10-2342 §9	Comply
25	Security per 33.401	10-79 §47	Comply
26	Support the optional security features specified in 3GPP TS 33.401 …“integrity protection and verification of data” and “ciphering/deciphering of data,” must be supported for signaling	10-2342 §25	Comply
27	either or both of IPv4/IPv6	10-2342 §13	Comply
Interoperability Testing (self-certification)			
28	Uu	10-79 §47	Comply
29	S1-U	10-79 §47	Comply
30	S1-MME	10-79 §47	Comply
31	S6a	10-2342 §19	Comply
32	S8	10-2342 §19	Comply
33	S9	10-2342 §19	Comply
34	Submit Interoperability plans to ERIC	10-79 §55	Comply
35	Certify vendor participation in PSCR	10-79 §61	Comply
36	Submit in quarterly report … a plan for conducting IOT on the interfaces	1079 §20	Comply
Applications			
37	Internet Access	10-79 §46	Comply
38	VPN Access to authorized sites and home networks	10-79 §46	Comply
39	Status or Information Homepage	10-79 §46	Comply
40	Access to responders under the Incident Command System	10-79 §46	Comply
41	Field-based Server applications	10-79 §46	Comply
RF Performance			

42	Require each Petitioner to implement the Static Inter-Cell Interference Coordination … by its date of service availability to ensure that the network operates without interference	10-2342 §26	Comply
43	Out Of Band Emissions	10-79 §44	Comply
44	provide outdoor coverage at minimum data rates of 256 Kbps uplink (UL) and 768 Kbps downlink (DL), for all types of devices, for a single user at the cell edge … based on a sector loading of seventy percent, throughout the entire network	10-2342 §22	Comply
45	achieve significant population coverage within its jurisdiction within ten years of its date of service availability.	10-2342 §23	Comply
46	require that Petitioners' systems provide a probability of coverage of 95 percent for all services and applications throughout the network as built.	10-2342 §24	Comply
47	PTCRB Certification	10-79 §47 10-2342 §18	Comply